Ochrona Danych Osobowych po zmianach unijnego Rozporządzenia o Danych Osobowych (RODO).

Dr Bartosz Mendyk

Fundusze Europejskie Program Regionalny
Rzeczpospolita Polska
promuje łódzkie
Unia Europejska Europejski Fundusz Społeczny

Historia wejścia w życie RODO

24-10-1995
- Uchwalenie dyrektywy 95/46/WE

29-08-1997
- Przyjęcie polskiej ustawy o ochronie danych osobowych-

04-11-2010
- Zainicjowanie kompleksowego podejścia do kwestii ochrony danych osobowych

25-01-2012
- Propozycja reformy

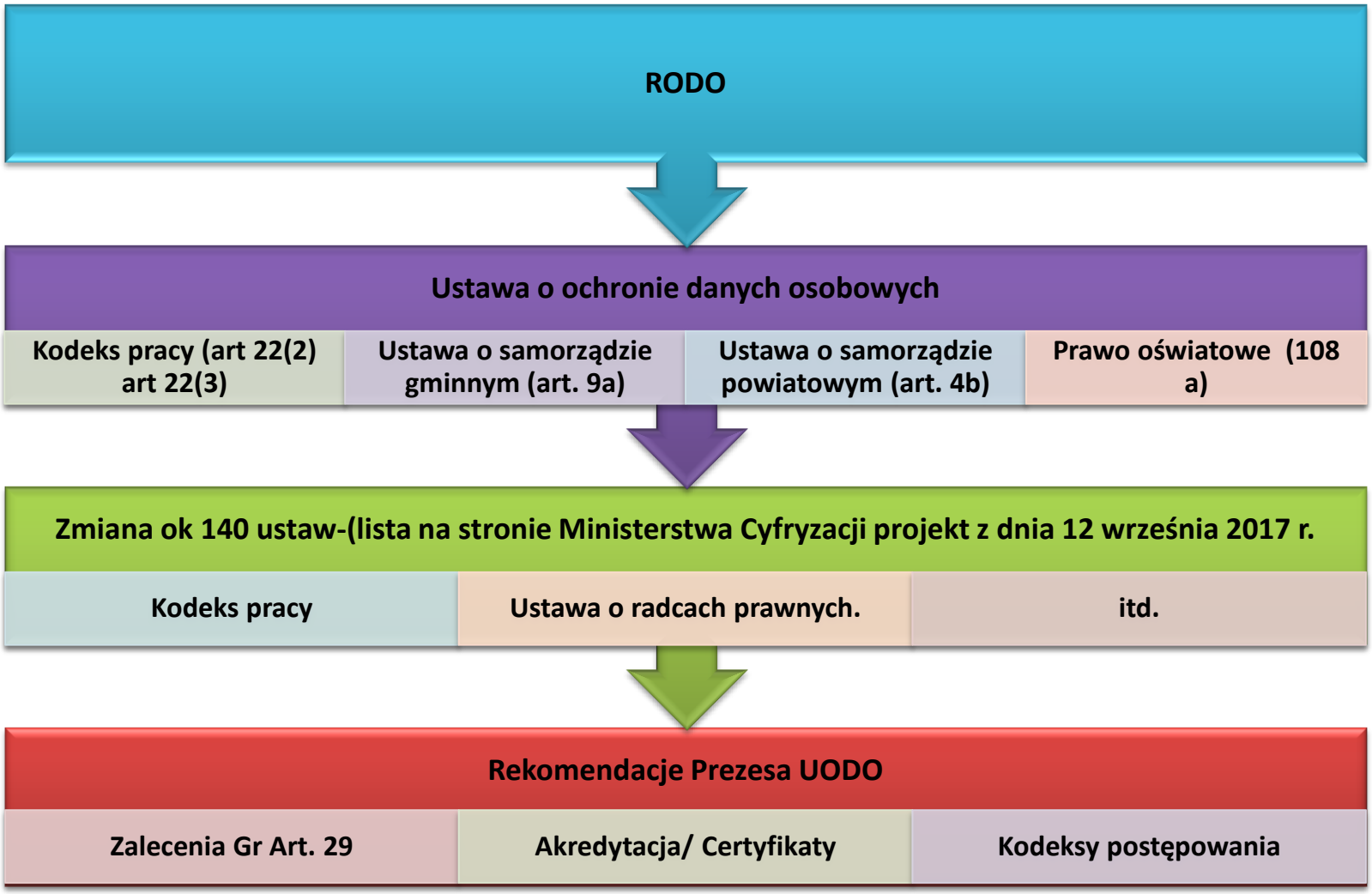
07-11-2014
- Ustawa o ułatwieniu wykonywania działalności gospodarczej

01-01-2015
- Wejście w życie ustawy

27-04-2016
- Uchwalenie RODO

25-05-2018
- Obowiązywanie RODO

1. Reforma przepisów o RODO Źródła prawa



V Filarów RODO

LEGALNOŚĆ

ŚWIADOMOŚĆ

ZABEZPIECZENIA

OBOWIĄZKI WZGLĘDEM REGULATORA (GIODO)

PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ

Definicje podobne

„dane osobowe” oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej

Dane wrażliwe vs szczególne kategorie danych

- **art. 27 ust. 1**
- – pochodzenie rasowe lub etniczne
- – poglądy polityczne
- – przekonania religijne lub filozoficzne
- – przynależność wyznaniowa, partyjna lub związkowa
- – życie seksualne

- – wyroki, orzeczenia o ukaraniu i mandatach karnych oraz inne wydane w postępowaniu sądowym lub administracyjnym
- Nałogi
- BRAK

- – stan zdrowia

- – kod genetyczny

- **art. 9 ust 1**
- – pochodzenie rasowe lub etniczne
- – poglądy polityczne
- – przekonania religijne lub światopoglądowe
- – przynależność do związków zawodowych
- – dane dotyczące seksualności lub orientacji seksualnej

- BRAK

- BRAK
- – dane biometryczne (**art. 4 pkt 14**)

- Dane dotyczące zdrowia **art. 4 pkt 15, motyw 35 preambuły**

- – dane genetyczne **art. 4 pkt 13, motyw 34**

Wyroki skazujące i naruszenia prawa

- art. 10 RODO– przetwarzanie danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa na podstawie art. 6 ust. 1 [Zgodność przetwarzania z prawem] **wolno dokonywać wyłącznie pod nadzorem władz publicznych** lub **jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą**. Wszelkie kompletne rejestry wyroków skazujących są prowadzone wyłącznie pod nadzorem władz publicznych.

Lista rzeczy do zrobienia w kategorii podstawowych definicji

Należy zidentyfikować dane w oparciu o nowy podział: dane zwykłe, szczególne kategorie danych, dane objęte specjalnymi warunkami przetwarzania

Należy się upewnić, że istnieją uzasadnione powody gromadzenia określonej kategorii danych w organizacji

Przetwarzanie danych

- **art. 4 pkt 2 RODO**
- *Na użytek niniejszego rozporządzenia:*
- *2) „przetwarzanie” oznacza **operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany**, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;*

Podstawy przetwarzania danych zwykłych art. 6

- osoba, której dane dotyczą wyraziła na to **zgodę**;
- jest niezbędne do wykonania **umowy** lub podjęcia działań przed jej zawarciem;
- jest niezbędne do wypełnienia **obowiązku prawnego**;
- jest niezbędne do **ochrony żywotnych interesów** osoby, której dane dotyczą, lub innej osoby fizycznej;
- jest niezbędne do wykonania **zadania realizowanego w interesie publicznym** lub w ramach **sprawowania władzy publicznej**;
- jest niezbędne do celów wynikających z **prawnie uzasadnionych interesów**.

- 3. Podstawa przetwarzania, o którym mowa w ust. 1 lit. c) i e), musi być określona:

- **a) w prawie Unii; lub**
- **b) w prawie państwa członkowskiego, któremu podlega administrator.**

Przetwarzanie szczególnych kategorii danych osobowych

- **1. Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.**

- 2. Ust. 1 nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków:
- a)osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1;
- **b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;**
- **c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;**
- e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
- f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
- g) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;
- h) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3;
- i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osoób, których dane dotyczą, w szczególności tajemnicę zawodową;
- j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

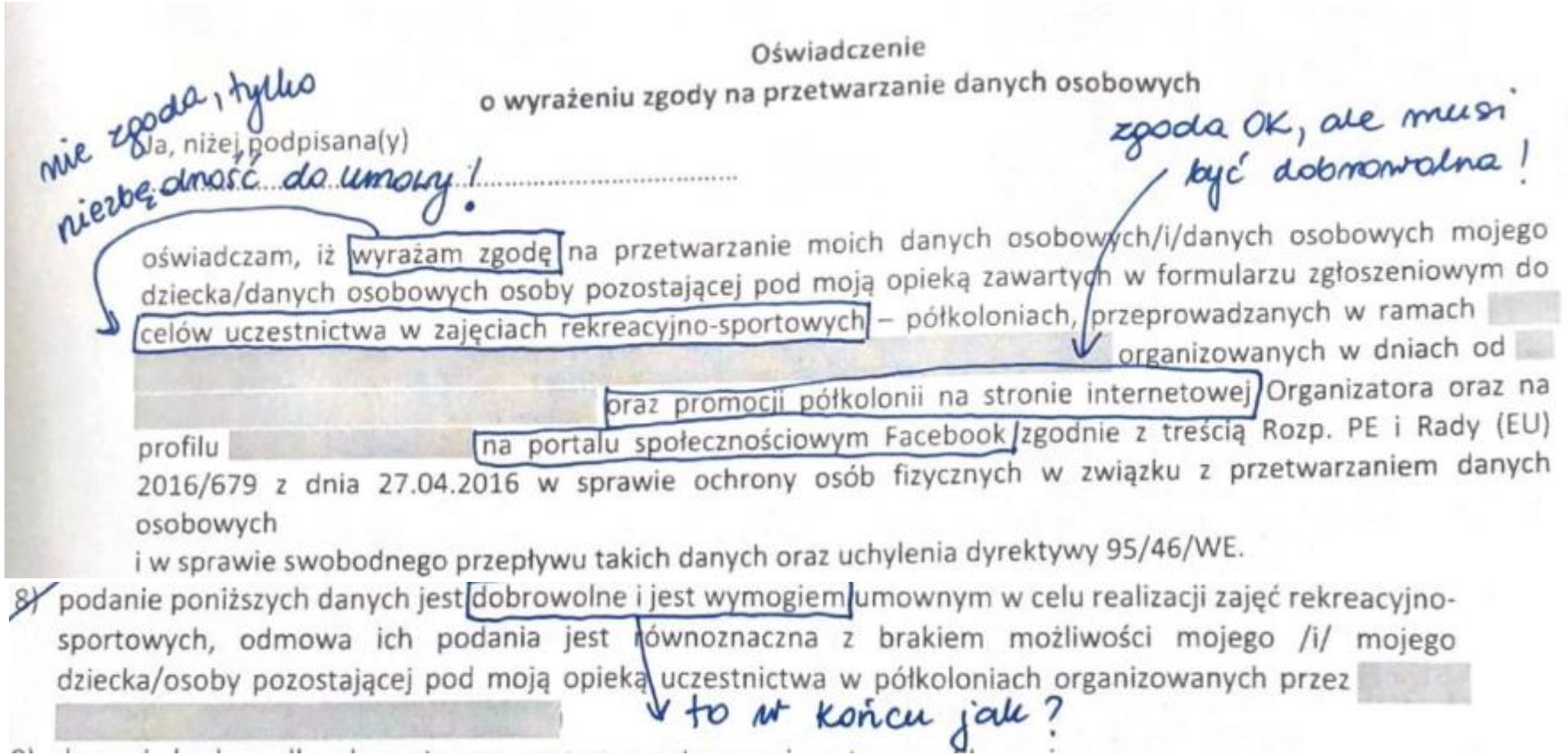
Przetwarzanie szczególnych kategorii danych osobowych - najważniejsze zmiany:

- Wprowadzenie nowego pojęcia „szczególnych kategorii danych osobowych” zamiast dotychczas funkcjonującego w polskiej literaturze pojęcia „danych wrażliwych”;
- Zniesienie wymogu zgody na piśmie (jako jednej z przesłanek przetwarzania tych danych);
- Dodanie do tej kategorii danych biometrycznych, np. układ linii papilarnych, owal twarzy, obraz siatkówki oka;
- Obowiązkowe powołanie Inspektora Ochrony Danych, przy przetwarzaniu na dużą skalę;
- Obowiązek przeprowadzenia tzw. oceny skutków dla ochrony danych (m. in. w przypadku przetwarzania na dużą skalę danych szczególnej kategorii);

Zgoda na przetwarzanie danych

- Zgoda osoby, której dane dotyczą **oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli**, którym osoba, której dane dotyczą, **w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych** (art. 4, pkt 11 RODO).
- **zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności**, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, których dane dotyczą, na przetwarzanie dotyczących jej danych osobowych i która ma na przykład **formę pisemnego (w tym elektronicznego) lub ustnego oświadczenia** (motyw 32 RODO).

zgody na przetwarzanie danych – przykłady



Oświadczenie

o wyrażeniu zgody na przetwarzanie danych osobowych

nie zgoda, tylko niezbędność do umowy!

zgoda OK, ale musi być dobrowolna!

Ja, niżej podpisana(y) .....

oświadczam, iż wyrażam zgodę na przetwarzanie moich danych osobowych/i/danych osobowych mojego dziecka/danych osobowych osoby pozostającej pod moją opieką zawartych w formularzu zgłoszeniowym do celów uczestnictwa w zajęciach rekreacyjno-sportowych – półkoloniach, przeprowadzanych w ramach [redacted] organizowanych w dniach od [redacted] oraz promocji półkolonii na stronie internetowej [redacted] Organizatora oraz na profilu [redacted] na portalu społecznościowym Facebook zgodnie z treścią Rozp. PE i Rady (EU) 2016/679 z dnia 27.04.2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

8) podanie poniższych danych jest dobrowolne i jest wymogiem umownym w celu realizacji zajęć rekreacyjno-sportowych, odmowa ich podania jest równoznaczna z brakiem możliwości mojego /i/ mojego dziecka/osoby pozostającej pod moją opieką uczestnictwa w półkoloniach organizowanych przez [redacted]

to w końcu jak?

- Źródło zdjęcia: Panoptykon

Przykłady zgód:

- portal internetowy pragnie zbierać informacje o lokalizacji swoich użytkowników i wykorzystywać je w celach marketingowych;
- Sklep typu dom i ogród chce wiedzieć, gdzie mieszkają jego klienci (więc pyta o kod pocztowy);
- organizacja społeczna chce przekazywać danych osobowe swoich beneficjentów partnerom z krajów poza UE aby Ci mogli je przetwarzać na własny użytek.

Wykorzystanie wizerunku

Art. 81. 1. Rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej. W braku wyraźnego zastrzeżenia zezwolenie nie jest wymagane, jeżeli osoba ta otrzymała umówioną zapłatę za pozowanie.

Pojęcie wizerunku jako „szczegółu całości" wiąże się z jego „akcydentalnym lub akcesoryjnym" charakterem, **zatem trzeba patrzeć, czy w razie jego usunięcia zmieni się całościowy obraz** (to znów z orzeczenia dotyczącego starych zdjęć klasowych — I ACa 1452/13);

2. Zezwolenia nie wymaga rozpowszechnianie wizerunku:

1) osoby powszechnie znanej, jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych;

2) osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza.

Określenie zgromadzenie dotyczy każdej zbiorowości, niezależnie czy jest ona przypadkowa czy zorganizowana. Jeśli więc wykonanie zdjęcia czy nagrania nie było ukierunkowane indywidualnie na określoną osobę, przeciwnie osoba ta jest przedstawiona w sposób równoważny przedstawieniu innych osób, to rozpowszechnianie takiego wizerunku nie wymaga zgody. Kwestionowane przez powoda zdjęcia, zawierające również wizerunek powoda, obrazują uczniów poszczególnych klas na różnych etapach edukacji, zdjęcia te nie są w żadnym stopniu ukierunkowane na powoda. Tym samym zarówno użytkownik portalu, który zdjęcie zamieścił, jak również pozwany świadczący usługę hostingową, nie byli zobligowani do uzyskania zgody powoda na opublikowanie zdjęcia m. in. z jego wizerunkiem.

ZGODY- Lista rzeczy do zrobienia

- **czy w przypadku zbierania zgody, jej wycofanie jest równie łatwe jak wyrażenie zgody;**
- **czy w prawidłowy sposób formułowane jest zapytanie o zgodę;**
- **Czy urząd jest w stanie wykazać uzyskanie zgody osoby, której dane dotyczą;**

OBOWIĄZEK INFORMACYJNY

Po 25 maja 2018 roku zakres obowiązku informacyjnego ulegnie znacznemu rozszerzeniu. Zgodnie z RODO administrator danych w przypadku pozyskiwania informacji od osoby, której one dotyczą będzie zobowiązany do podania:

- swojej tożsamości, pełnej nazwy i danych kontaktowych;
- danych kontaktowych IOD (jeżeli został powołany);
- celu i **podstawy przetwarzania danych osobowych;**
- prawnie uzasadnionego interesu/-ów administratora danych (jeżeli takowy istnieje);
- informacji o odbiorcach danych osobowych lub o kategoriach odbiorców;
- informacji o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
- okresu przechowywania danych;
- informacji o prawach podmiotu (dostęp do danych, ich przenoszenie, sprzeciw, sprostowanie, usunięcie etc.);
- informacji o prawie do cofnięcia zgody;
- informacji o prawie do wniesienia skargi do organu nadzorczego;
- **informacji czy podanie danych to wymóg ustawowy lub umowny lub warunek zawarcia umowy oraz konsekwencji nie podania danych;**
- **informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu** (w tym o zasadach podejmowania, znaczeniach i konsekwencjach).

PRAWA PODMIOTÓW DANYCH

Zgodnie z brzmieniem rozporządzenia, od 25 maja 2018 roku podmioty danych zostaną wyposażone w uprawnienia, takie jak:

- „**Prawo do bycia zapomnianym**” – podmiot danych ma prawo zażądać od administratora niezwłocznego usunięcia jego danych osobowych, jeżeli zajdzie jedna z enumeratywnie wymienionych okoliczności z art. 17 ust. 1 pkt. a-f RODO.
- **Prawo do sprostowania danych** – podmiot ma prawo żądać od administratora danych niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Instytucja ta obecna jest już w polskich przepisach.
- **Prawo do ograniczenia przetwarzania** – osoba, które dane dotyczą ma prawo żądania od administratora danych ograniczenia przetwarzania jej danych osobowych w przypadkach wymienionych w art. 18 ust. 1 pkt. a-d RODO.
- **Prawo do przenoszenia danych** – osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora.
- **prawo do niepodlegania przez konkretną osobę fizyczną decyzjom wywołującym wobec niej skutki prawne lub podobnie wpływającym na nią w inny istotny sposób**.

- W związku z rozszerzeniem katalogu praw przysługujących podmiotom danych należy przygotować i implementować w realizację:
  - Prawa do sprostowania danych;
  - Prawa do ograniczenia przetwarzania danych ;
  - Prawa do przeniesienia danych.

Prawo do usunięcia danych („prawo do bycia zapomnianym”)

- Historia: C-131/12 (Google Spain), w którym TSUE rozstrzygnął, że każdemu internaucie służy prawo do bycia zapomnianym. **Orzeczenie nie nakazuje usuwania danych źródłowych ze stron, a wyłącznie odnośniki (linki) do nich, które indeksuje i publikuje wyszukiwarka.**

- Przesłanki powstania:

- 1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
- 2) osoba, której dane dotyczą, cofnęła zgodę, na której opierało się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
- 3) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania dotyczących jej danych osobowych:
- a) z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na interesie publicznym lub prawnie uzasadnionych interesach i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania; lub
- b) wobec przetwarzania jej danych osobowych na potrzeby marketingu bezpośredniego;
- 4) dane osobowe były przetwarzane niezgodnie z prawem;
- 5) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;
- 6) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 GDPR.

- Wyjątki
- 1) do korzystania z prawa do wolności wypowiedzi i informacji;
- 2) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- 3) z uwagi na:
- a) cele zdrowotne; oraz
- b) interes publiczny w dziedzinie zdrowia publicznego;
- 4) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub
- 5) do ustalenia, dochodzenia lub obrony roszczeń.

Udostępnienie danych

- Podmiot, któremu dane zostały udostępnione staje się ich administratorem, ponieważ jest w stanie samodzielnie decydować o celu i sposobie przetwarzania tych danych.

Udostępnienie

- Powierzający dane osobowe ustala cel, zakres i sposób przetwarzania. Przekazując dane nie traci statusu Administratora Danych.
- Podmiot przyjmujący dane w powierzenie nie staje się ich administratorem (jest ograniczony co do celu i zakresu przetwarzania otrzymanych danych).

Powierzenie

Udostępnienie

- udostępnienie danych policji
- sądowi
- firmie ubezpieczeniowej

Powierzenie

- serwis komputerów
- serwis oprogramowania
- archiwizacja danych
- obsługa kadrowo-płacowa

Przepisy Zagadnienie	UODO	RODO
Podstawa prawna	• art. 31	• art. 28
Forma umowy	• forma pisemna	• forma pisemna, w tym forma elektroniczna
Elementy umowy	• zakres danych osobowych • cel przetwarzania	• przedmiot • czas trwania powierzenia • charakter i cel przetwarzania • rodzaj danych osobowych • kategorie osób, których dane dotyczą • warunki podpowierzenia przetwarzania danych • obowiązki i prawa administratora danych • obowiązki procesora
Podpowierzenie	• brak regulacji	• pisemna zgoda administratora danych (szczegółowa lub ogólna)

Umowa powierzenia przetwarzania danych osobowych

- Zgodnie z art. 28 *rodo*, umowa powierzenia powinna określać: **przedmiot** i **czas** trwania przetwarzania, **charakter** i **cel** przetwarzania, **rodzaj danych** osobowych, **kategorie osób**, których dane dotyczą, **obowiązki i prawa administratora**, a także **obowiązki procesora**, których przykładowe wyliczenie zawiera ustęp 3 wskazanego artykułu.

- Oprócz wymogu szczegółowego opisu procesu powierzenia przetwarzania danych, *rodo* wskazuje również obowiązki procesora, których wyliczenie powinno znaleźć się w zawieranej umowie (art. 28 ust. 3 pkt a)-h) *rodo*). Zaliczymy do nich m.in.:
- **przetwarzanie danych osobowych wyłącznie na udokumentowane polecenie administratora,**
- **zapewnienie, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,**
- **podejmowanie wymaganych środków zabezpieczających przetwarzane dane osobowe,**
- **pomoc administratorowi w wywiązywaniu się z obowiązków wobec osób, których dane dotyczą,**
- **po zakończeniu świadczenia usług związanych z przetwarzaniem, usunięcie lub zwrot wszelkie dane osobowe oraz usunięcie ich istniejących kopii (zależnie od decyzji administratora).**

Obowiązek sporządzenie rejestru czynności przetwarzania

- Obowiązek rejestrowania **nie ma zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób**.
- Podmiot będzie musiał prowadzić wtedy gdy:
  - przetwarzanie **może powodować ryzyko naruszenia praw lub wolności osób**, których dane dotyczą,
  - **nie ma charakteru sporadycznego** lub
  - **obejmuje szczególne kategorie danych osobowych**.

Rejestr czynności przetwarzania zawiera:

- **nazwę i dane kontaktowe administratora danych oraz dane kontaktowe IOD jeżeli został powołany**,
- **cel przetwarzania danych osobowych,**
- opis kategorii osób, których dane dotyczą oraz zakres danych (wrażliwe lub zwykłe),
- **kategorie odbiorców, którym dane zostały lub zostaną udostępnione**,
- informację o przekazywaniu danych do państwa trzeciego wraz z dokumentacją opisującą zastosowane zabezpieczenia w tym procesie,
- **planowany termin usunięcia danych osobowych,**
- **ogólny opis zastosowanych zabezpieczeń technicznych i organizacyjnych**.

Fundusze Europejskie Program Regionalny
Rzeczpospolita Polska
promuje łódzkie
Unia Europejska Europejski Fundusz Społeczny

Ocena skutków dla ochrony danych

RODO, w art. 35 ust. 3 przedstawia przykłady przypadków, gdy przetwarzanie *„z dużym prawdopodobieństwem może powodować wysokie ryzyko*”. Będzie to przetwarzanie wymagające:

- *- „(a) **systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych**, która opiera się na **zautomatyzowanym przetwarzaniu**, w tym **profilowaniu**, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;*
- *- (b) przetwarzania na dużą skalę **szczególnych kategorii danych osobowych**,(…) lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa (…)*
- *- (c) **systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie**.”*
- *(gr art. 29) **Dane dotyczące osób, których dane dotyczą, wymagających szczególnej opieki***
- ***Gdy UODO tak określi***
- Nie robimy gdy: **Oceny skutków dokonano już w ramach oceny skutków regulacji w związku z przyjęciem podstawy prawnej przetwarzania danych w prawie Unii lub w prawie krajowym.**

Co składa się na DPIA?

- - elastyczność struktury i formy
- Art. 35 ust 7 (+ Motyw 84 i 90) Ocena zawiera co najmniej:
- a) **systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie** – prawnie uzasadnionych interesów realizowanych przez administratora;
- b) **ocenę, czy operacje przetwarzania są niezbędne** oraz proporcjonalne w stosunku do celów;
- c) **ocenę ryzyka naruszenia praw lub wolności osób,** których dane dotyczą, o którym mowa w ust. 1; oraz
- d) **środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzeni**a, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

- **Organy nadzorcze mają tworzyć i podawać do publicznej wiadomości wykazy rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych, jak również wykazy operacji, które takiemu obowiązkowi nie podlegają.**

Procedura oceny ryzyka

- Art 24. ust. 1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.
- Art. 32. 2. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, **uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych**.

Privacy by default/ Privacy by design

- **uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania**, administrator – **zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania –wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych**, takich jak **minimalizacja danych**, oraz **w celu nadania przetwarzaniu niezbędnych zabezpieczeń**, tak by **spełnić wymogi niniejszego rozporządzenia** oraz **chronić prawa osób**, których dane dotyczą (art. 25 ust 1 RODO).
- **administrator wdraża odpowiednie środki techniczne i organizacyjne**, aby **domyślnie przetwarzane były wyłącznie te dane osobowe**, **które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania**. **Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności**.

Inspektor Ochrony Danych powołanie

- **a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;**

- b) główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub

- c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10

Inspektor ochrony danych

Art. 9. Przez organy i podmioty publiczne obowiązane do wyznaczenia inspektora (…) rozumie się:

- 1) jednostki sektora finansów publicznych;
- 2) instytuty badawcze
- 3) Narodowy Bank Polski.

Podmiot, który wyznaczył inspektora, zawiadamia Prezesa Urzędu o jego wyznaczeniu w terminie 14 dni od dnia wyznaczenia, wskazując imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora.

W przypadku wyznaczenia jednego inspektora przez organy lub podmioty publiczne albo przez grupę przedsiębiorców, każdy z tych podmiotów dokonuje zawiadomienia

Zawiadomienia, o których mowa w ust. 1 i 4, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.

Inspektor Ochrony Danych

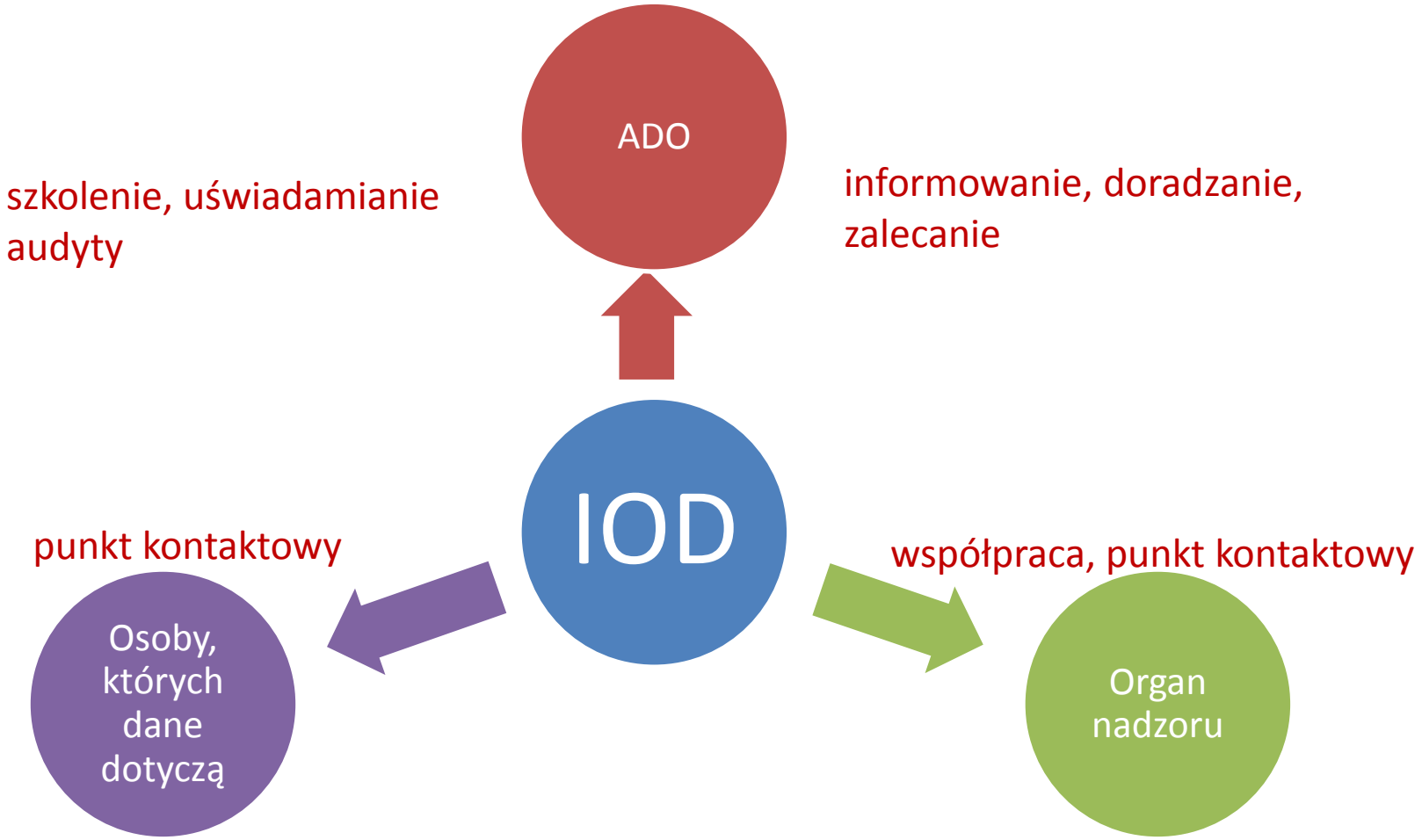
Kwalifikacje do pełnienia funkcji

- Zgodnie z art. 37 ust. 5 RODO inspektor ochrony danych jest **wyznaczany na podstawie kwalifikacji zawodowych**, a w szczególności **wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych** oraz **umiejętności wypełnienia zadań**, o których mowa w art. 39 RODO. Poziom wiedzy inspektora powinien być ustalany w kontekście konkretnych potrzeb administratora danych i procesora (motyw 97 RODO).

Gwarancje niezależności

- **ma podlegać bezpośrednio najwyższemu kierownictwu administratora lub podmiotu przetwarzającego**
- **ma podlegać bezpośrednio najwyższemu kierownictwu administratora lub podmiotu przetwarzającego**
- zakazu wydawania przez administratora lub podmiotu przetwarzającego instrukcji (poleceń) dla DPO dotyczących wykonywania przez niego zadań
- Zgodnie z art. 38 ust. 6 RODO, istnieje możliwość nakładania na inspektora ochrony danych innych zadań i obowiązków, ale administrator i podmiot przetwarzający muszą zapewnić by nie powodowało to konfliktu interesów
- Zakaz odwoływania i karania DPO
- Obowiązek zachowania tajemnicy lub poufności co do wykonywania zadań przez DPO

IOD Zadania


ADO
szkolenie, uświadamianie
audyty
informowanie, doradzanie,
zalecanie
IOD
punkt kontaktowy
współpraca, punkt kontaktowy
Osoby,
których
dane
dotyczą
Organ
nadzoru

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

- **Natychmiast po stwierdzeniu naruszenia ochrony danych osobowych administrator powinien zgłosić je organowi nadzorczemu bez zbędnej zwłoki, jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, chyba że administrator jest w stanie wykazać zgodnie z zasadą rozliczalności, że jest mało prawdopodobne, by naruszenie to mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych**. Jeżeli nie można dokonać zgłoszenia w terminie 72 godzin, zgłoszeniu powinno towarzyszyć wyjaśnienie przyczyn opóźnienia, a informacje mogą być przekazywane stopniowo, bez dalszej zbędnej zwłoki.

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

- **a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;**
- **b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;**
- **c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;**
- **d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.**
- Punkt kontaktowy- nie oznacza pełnomocnika upoważnionego do reprezentowania spółki, a optymalny dla administratora sposób kontaktu z Prezesem Urzędu Danych Osobowych.

Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

- Tak jak w przypadku obowiązku informacyjnego również tutaj nadrzędnym obowiązkiem jest jasność przekazu- tak aby podmiot danych osobowych mógł zrozumieć, jakie to było naruszenie. Dlatego **zawiadomienie, językiem jasnym i prostym opisuje charakter naruszenia ochrony danych osobowych** oraz zawiera przynajmniej informacje, które zawierają (art. 34, który odsyła do : art. 33. Ust. 1 lib b, c, d):
- b) **zawiera imię i nazwisko oraz dane kontaktowe inspektora ochrony danych** lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- c) **opisują możliwe konsekwencje naruszenia ochrony danych osobowych**;
- d) **opisują środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych**, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

INSPEKTOR OCHRONY DANYCH

W związku ze zmianami w zakresie obowiązku powołania oraz funkcjonowania IOD rekomenduję:

- Rozważenie outsourcingu funkcji IOD.
- Wybór odpowiedniej osoby na stanowisko IOD i umiejscowienie jej w strukturze.
- Opracowanie procedury wyboru IOD.
- Przygotowanie szkoleń lub webinarium z zakresu przetwarzania danych.
- Opracowanie procedur działa IOD (m.in. zgłaszania naruszeń ochrony danych osobowych do organu nadzorczego lub kontaktu podmiotów danych z IOD).

Świadomość

Obecnie

- Szkolenia
- Budowanie świadomości zagrożeń i odpowiedzialności

RODO

- Szkolenia organizowane przez IOD lub administratora danych
- Budowanie świadomości zagrożeń i odpowiedzialności
- Privacy by default, privacy by design:udział IOD już na etapie projektowania rozwiązań przetwarzania danych
- Świadomość roli IOD w organizacji

Zabezpieczenia

Obecnie

- Zabezpieczenia techniczne (IT oraz fizyczne)
- Zabezpieczenia organizacyjne (polityka bezpieczeństwa, instrukcja zarządzania, wyznaczenie ABI, ASI)

RODO

- Zabezpieczenia IT wg wewnętrznych polityk lub wytycznych regulatora
- Zabezpieczenia organizacyjne (polityka bezpieczeństwa, wyznaczenie IOD)
- Ocena skutków dla ochrony danych
- Deregulacja: regulator wydaje zalecenia i wzory dobrych praktyk
- Certyfikacja i kodeksy postępowania
- Rejestrowanie czynności przetwarzania

Obowiązki wobec Regulatora

Obecnie

- zbiorów danych
- Zgłaszanie ABI

RODO

- Zgłaszanie incydentów
- Konsultowanie innowacyjnych procesów z regulatorem
- Zgłaszanie IOD
- Uwzględnianie wytycznych i zaleceń

Elementy na jakie należy zwrócić uwagę przy wrażaniu RODO

- Zgoda na przetwarzanie danych osobowych;
- Obowiązek informacyjny;
- Inspektor Danych Osobowych;
- Nowe prawa podmiotów danych;
- Rejestr czynności przetwarzania danych;
- Zgłaszanie naruszeń ochrony danych osobowych;
- Powierzania przetwarzania danych;
- Kodeksy i certyfikaty zgodności przetwarzania danych.

Przykładowe problemy w praktycznym stosowaniu ochrony danych osobowych i występujące zagrożenia

- Nadużywanie zgód- “zgoda na wszystko” lub “zgoda bije wszystko”
- błędne zinterpretowanie podstaw przetwarzania
- Oświadczam, że zapoznałem się z obowiązkiem informacyjnym.
- Podpisywanie ze wszystkimi umów powierzenia.

Potencjalna lista wszelkich nowych dokumentów vs. Wymagania RODO

- Procedura współpracy z organem nadzoru
- Przeprowadzenie oceny skutków dla ochrony danych
- Procedura realizacji prawa do sprostowania danych,
- Procedura realizacji prawa do usunięcia danych
- Procedura realizacji prawa do ograniczonego przetwarzania
- Procedura realizacji prawa do przenoszenia danych
- Procedura realizacji prawa do sprzeciwu
- Formularze do zgłoszenia naruszenia bezpieczeństwa.
- Dokumenty dla DPO
- Wzór umowy o powierzenie danych do przetwarzania
- Wzór rejestru czynności przetwarzania danych
- Dokumenty do stosowania procedury privacy by design.
- Dokumenty do stosowania procedury privacy by default
- Procedura weryfikacji podmiotu, któremu dane są powierzane do przetwarzania.

- prowadzenie rejestru czynności przetwarzania i zakres rejestru kategorii czynności przetwarzania, o których mowa w art. 30 RODO;
- zgłaszanie naruszenie ochrony danych do organu nadzorczego (UODO) – art. 33 ust 3 RODO;
- prowadzenie wewnętrznej dokumentacji stanowiącej rejestr naruszeń ochrony danych, o którym mowa w art. 33 ust 5 RODO;
- zawartość raportu dokumentującego wyniki przeprowadzonych ocen skutków dla ochrony danych – art. 35 ust. 7.

Dotychczasową dokumentacją należy uzupełnić o:

rejestr czynności przetwarzania i zakres rejestru kategorii czynności przetwarzania, o których mowa w art. 30 RODO;

wytyczne dotyczące klasyfikacji naruszeń i procedurę zgłaszanie naruszenie ochrony danych do organu nadzorczego (UODO) – art. 33 ust 3 RODO;

procedurę na wypadek wystąpienia naruszeń mogących powodować wysokie ryzyko naruszenia praw i wolności osób, w zakresie ich informowaniu o działaniach jakie powinni wykonać, aby ryzyko to ograniczyć – art. 34 RODO

procedurę prowadzenia wewnętrznej dokumentacji stanowiącej rejestr naruszeń ochrony danych, o którym mowa w art. 33 ust 5 RODO;

raport z przeprowadzonej, ogólnej analizy ryzyka; raport z ocen skutków dla ochrony danych – art. 35 ust. 7. – jeśli dotyczy;

procedury związane z pseudonimizacją i szyfrowaniem – jeśli dotyczy; plan ciągłości działania – art. 32 ust 1 pkt b RODO;

procedury odtwarzania systemu po awarii, oraz ich testowania – art. 32 ust 1 pkt c i d RODO

Dokumentacja RODO (opinia UODO)

RODO nie wymaga jednak, aby dokument zawierający wymienione wyżej, obligatoryjne elementy dokumentacji miał określona nazwę, czy strukturę.

Ważne jest tylko, aby administrator danych wykazał, że wymienione wyżej rejestry, czy raporty posiadał i aby ich zawartość była zgodna z wskazanymi wyżej wymaganiami tj. wymaganiami wskazanymi odpowiednio w art. 30, art. 33 ust 3 i 5 oraz art. 35 ust 7 RODO.

W praktyce oznacza to, że administrator ma obowiązek wykazać, że:

a.) stosuje się do ogólnych zasad przetwarzania określonych w art. 5 RODO,

b.) zapewnia, aby dane przetwarzane były zgodnie z prawem – art. 6 – 11 RODO,

c.) zapewnia, aby przestrzegane były prawa osób, których dane są przetwarzane – art. 12-23 RODO

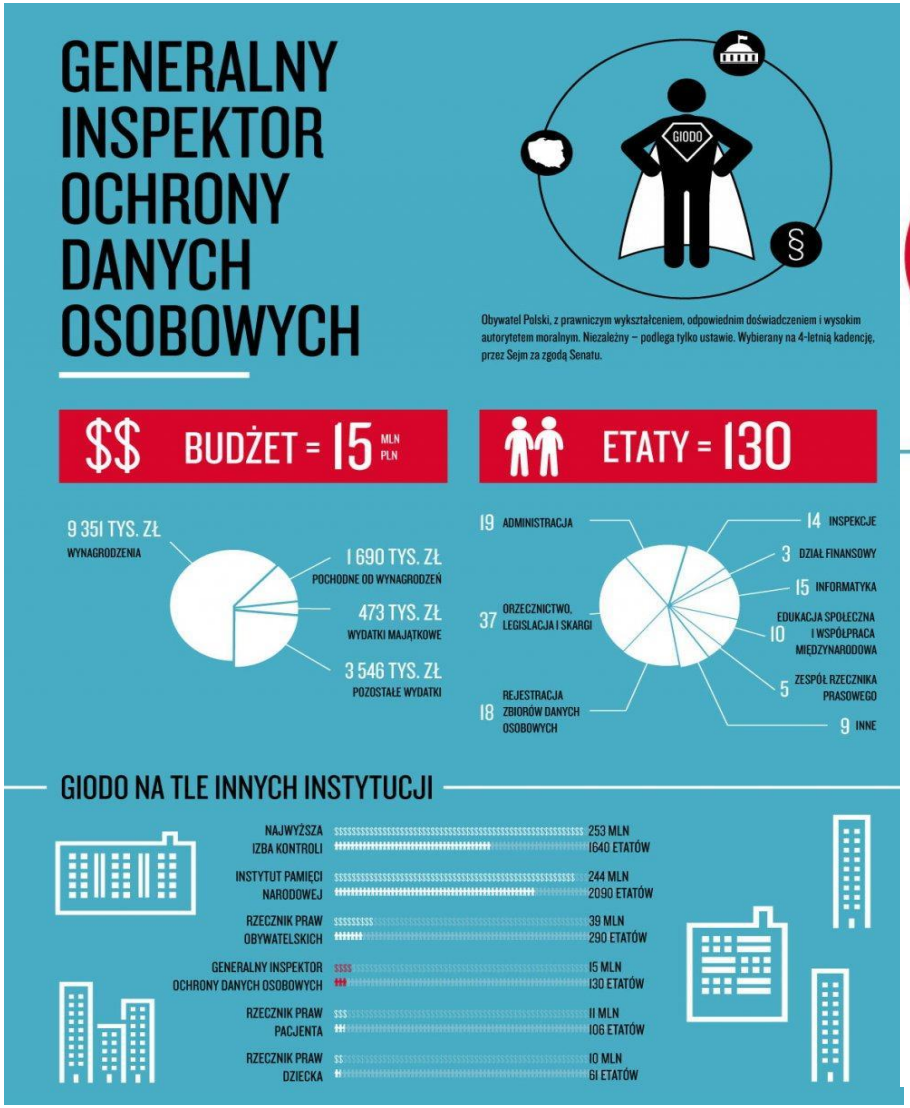
d.) zapewnia wypełnianie ogólnych obowiązków w zakresie przetwarzania danych ciążących na administratorze i podmiocie przetwarzającym – art. 24 – 31 RODO,

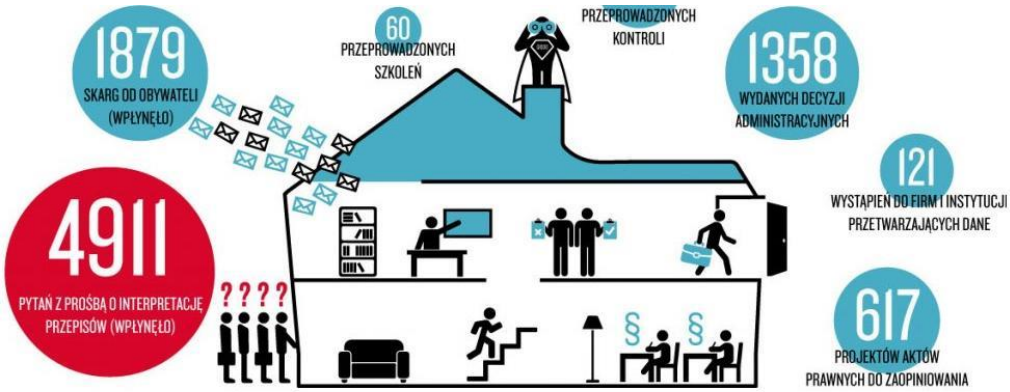
e.) zapewnia bezpieczeństwo przetwarzania danych uwzględniając charakter zakres, kontekst i cele przetwarzania danych – art. 32- 36 RODO,

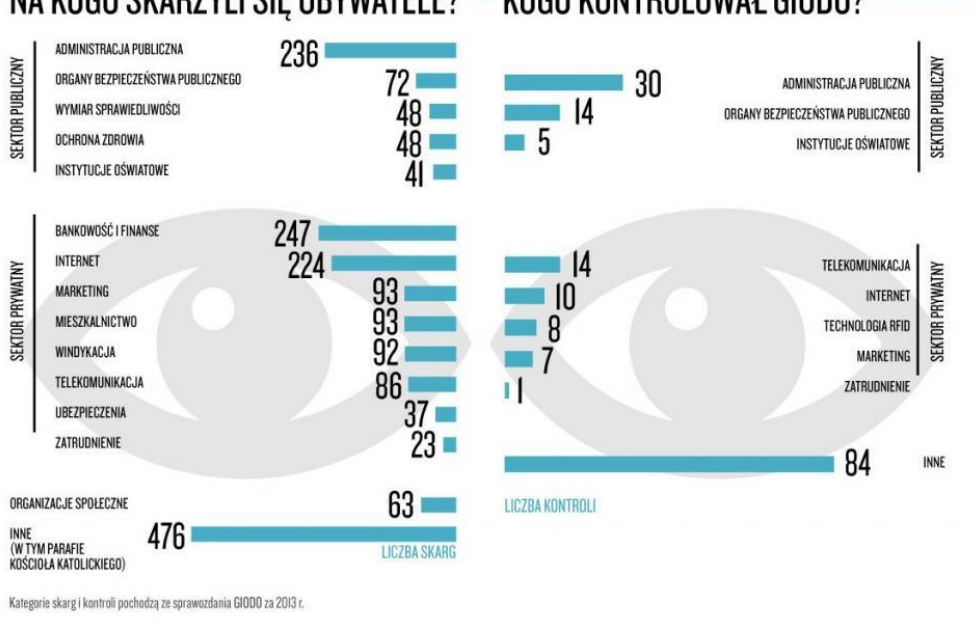
f.) zapewnia kontrolę nad przetwarzaniem danych w postaci monitorowanie przestrzegania przepisów i przyjętych procedur przetwarzania przez Inspektora Ochrony Danych lub podmioty certyfikujące, czy monitorujące przestrzeganie przyjętych kodeksów postepowania – art. 27- 43,

g.) stosuje się do wymagań w zakresie przekazywania danych do państw trzecich i instytucji międzynarodowych – art. 44 – 49 RODO.

Kontrole







Źródło: www.panoptykon.org

Przepisy o administracyjnych karach pieniężnych i przepisy karne

Art. 102. 1. Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 100 000 złotych, na:

- 1) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1–12 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych;
- 2) instytut badawczy;
- 3) Narodowy Bank Polski.

2. Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 10 000 złotych na jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.

Przepisy karne

Art. 107. 1. Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.

2. Jeżeli czyn określony w ust. 1 **dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.**

Art. 108. Kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.

Odpowiedzialność cywilna i postępowanie przed sądem

Art. 92. W zakresie nieuregulowanym rozporządzeniem 2016/679, do roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych, o których mowa w art. 79 i art. 82 tego rozporządzenia, stosuje się przepisy ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny.

Właściwy jest sąd okręgowy

Dziękujemy za uwagę!